Обзор расширений external_id_hash и external_session_id протокола TLS 1.3 (RFC 8844)

Автор: Садовский Антон

Проблема внешней идентификации и атак unknown key-share

В традиционном TLS аутентификация сторон осуществляется на основе сертификатов и параметров, передаваемых непосредственно в ходе TLS-рукопожатия. Однако в ряде протоколов, таких как WebRTC или SIP, идентификация участников или параметры сессии определяются вне TLS – через внешние сигнальные каналы.

Если злоумышленник получает возможность подменить данные во внешнем сигнальном канале, он может заставить одну из сторон установить TLS-соединение с неверным партнёром, при этом криптографические проверки TLS будут успешно пройдены. Такая ситуация называется атакой unknown key-share.

Для решения данной проблемы в RFC 8844 были определены два расширения TLS: external_id_hash и external_session_id. Эти расширения предназначены для криптографической привязки внешних идентификаторов и параметров сессии к TLS-рукопожатию.

Расширение external_id_hash

Расширение external_id_hash предназначено для передачи в рамках TLS-рукопожатия хэшированного значения внешних идентификационных данных. Основная цель расширения – обеспечить криптографическую привязку внешней учётной записи к TLS-сессии и предотвратить подмену участника соединения.

Перед установлением TLS-соединения каждая сторона получает внешнюю идентификационную информацию, например, идентификатор участника или данные о его сертификате. Из этой информации вычисляется хэш-значение с использованием алгоритма SHA-256.

Полученный хэш включается в расширение external_id_hash, которое передаётся клиентом в сообщении ClientHello, а сервером – в ответном

собщении. В ходе рукопожатия каждая сторона проверяет, совпадает ли полученный хэш с ожидаемым значением. При несовпадении TLS-соединение немедленно прерывается.

Таким образом, TLS-соединение становится криптографически связанным с внешней учётной записью. Даже если злоумышленник получает возможность изменить идентификационные данные во внешнем канале, он не сможет незаметно внедриться в TLS-соединение, так как несоответствие хэш-значений будет обнаружено на этапе рукопожатия.

Расширение external_session_id

Расширение external_session_id предназначено для передачи в рамках TLS-рукопожатия уникального идентификатора сессии, который формируется и используется вне протокола TLS. В отличие от external_id_hash, это расширение связывает TLS-рукопожатие не с учётной записью участника, а с конкретной логической сессией.

Расширение применяется в системах, где одновременно может существовать несколько TLS-соединений, управляемых одним сигнальным механизмом, и требуется исключить их взаимную подмену.

До начала TLS-рукопожатия внешний протокол формирует уникальный идентификатор сессии. Этот идентификатор может представлять собой случайную строку, числовое значение или иной уникальный маркер. Формат и способ генерации данного идентификатора полностью определяются прикладным уровнем.

Клиент включает полученный идентификатор в расширение external_session_id и передаёт его в сообщении ClientHello. Сервер, получив ClientHello, проверяет соответствие идентификатора ожидаемому значению и, в случае успеха, возвращает то же самое значение в своём ответе.

В процессе рукопожатия обе стороны выполняют проверку полученного идентификатора. Если значение совпадает с ожидаемым, TLS-рукопожатие продолжается и соединение считается корректно связанным с внешней сессией. При обнаружении несоответствия TLS-соединение немедленно

завершается, так как это указывает на попытку подмены, ошибку маршрутизации или нарушение целостности сигнального механизма.

Заключение

Основная практическая ценность расширений external_id_hash и external_session_id заключается в том, что они:

- устраняют разрыв между TLS и прикладным уровнем;
- делают атаки на сигнальные каналы бесполезными за счёт криптографической привязки к внешним данным;
- повышают безопасность систем реального времени без изменения базового протокола TLS.

Это позволяет безопасно использовать TLS в системах с внешней идентификацией участников.